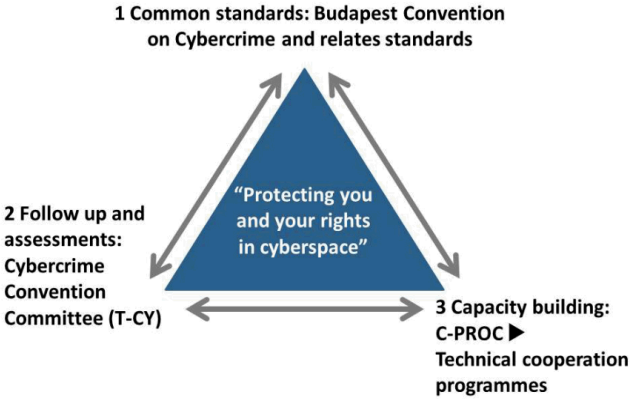
Cybercrime Division of the Council of Europe

The Council of Europe (CoE) helps to protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and capacity building programmes on cybercrime.

1 – The Budapest Convention

The Budapest Convention (or Cybercrime Convention) is the most relevant international treaty on cybercrime and electronic evidence. The treaty requires Parties to (a) establish a list offences against and by means of computers in their criminal law, (b) provide law enforcement with the powers to secure specified computer data in specific criminal investigations and in relation to any criminal offence, (c) limit such powers through rule of law safeguards and (d) engage in efficient international police-to-police and judicial cooperation, including through a 24/7 network of contact points.

All but two of the 47 member States of the Council of Europe (the exceptions being the Russian Federation and San Marino) including all members of the European Union are parties or have at least signed it. However, its geographical reach goes far beyond Europe. At present 66 States are either parties (the latest being Canada, Liechtenstein and Sri Lanka), signatories or have been invited to accede. At least double that number has used the Budapest Convention as a guideline for domestic legislation.



The Convention is more than the text of a treaty. It is this "dynamic triangle" of common standards, follow up and assessments, and capacity building which makes the difference.

2 – The Cybercrime Convention Committee (T-CY)

The T-CY represents the State Parties to the Budapest Convention on Cybercrime and is based on article 46 of the Convention. It comprises currently 66 parties and observer States as well as European Commission, EUROPOL, EUROJUST, INTERPOL, the UN Office on Drugs and Crime and other relevant organisations. The Committee assesses implementation of the treaty in practice, adopts Guidance Notes and may also prepare additional Protocols to the Convention. This Committee is probably the most relevant inter-governmental body on cybercrime internationally. The plenaries of the Cybercrime Convention Committee are organised twice per year and held in closed session.

The T-CY is also exploring solutions to address new challenges. A major challenge is criminal justice access to data – and thus evidence – in the cloud. The dilemma is that while law enforcement rules are tied by the principle of territoriality, data may be held temporarily or in parts by multiple layers of cloud service providers in various jurisdictions. It is often questionable how law enforcement authorities can legally access evidence in this context.

In the absence of clear international rules, government increasingly take unilateral action. The result is a jungle of approaches with risks for state-to-state relations and the rights of individuals.

The Cybercrime Convention Committee therefore established a "Cloud Evidence Working Group" to identify solutions. Specific proposals should become available in the course of 2016 and are to be presented at the Octopus Conference on Cybercrime, Strasbourg, 16 - 18 November 2016.
More on cloud evidence and the rule of law in cyberspace : http://europesworld.org/2015/12/07/evidence-cloud-rule-law-cyberspace/#.VrG82Wf2aUk (article by A.Seger, CoE).

3 – C-PROC

The Cybercrime Programme Office (C-PROC) of the CoE based in Bucharest, Romania, is responsible for assisting countries worldwide in the strengthening of their criminal justice capacity to respond to the challenges posed

by cybercrime and electronic evidence on the basis of the standards of the Convention. C-PROC, with its capacity building function, complements the work of the T-CY through which State Parties follow the implementation of the Budapest Convention (e.g. training of judges, establishment of specialised cybercrime units, improvement of interagency cooperation, protecting children against sexual violence online…). As a "Glazy glass process", cooperation between the CoE and third countries can acts as a "proxy" for a whole region.

C-PROC ongoing projects:

- GLACY (2013-2016): (Global Action on Cybercrime) is a joint project of the EU and CoE aimed at supporting countries worldwide in the implementation of the Budapest Convention. The specific objective of GLACY is: "to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime."
- CyberCrime Octopus: project based on voluntary contributions aimed at assisting countries worldwide to implement the Budapest Convention on Cybercrime and strengthen data protection and rule of law safeguards
- CyberCrimeEAP II and III: implemented within the EU and CoE Programmatic Cooperation Framework in the Eastern Partnership Countries aiming to optimize the regional and international cooperation on cybercrime and electronic evidence / and improving the cooperation between criminal justice authorities and service providers in specific criminal investigations and with the necessary rule of law safeguards.
- iPROCEEDS: Joint EU and CoE project to strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.